Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-60. (canceled)

61. (new) A processing system comprising:

a processor to support an isolated execution mode, a normal execution mode, a first privilege ring within the normal execution mode for use by an operating system (OS) kernel, and a second privilege ring within the normal execution mode for use by a software application;

a memory responsive to the processor, the memory to include an isolated memory area, the isolated memory area to be inaccessible to the processor in the normal execution mode;

a chipset responsive to the processor, the chipset to support the normal execution mode and the isolated execution mode;

processor executive (PE) handler storage in the chipset to store at least part of a PE handler, the PE handler to be loaded into the isolated memory area during a boot process for the processing system after at least a portion of the processing system is initialized, the PE handler to manage, from the isolated execution mode, at least one subsequent operation in the boot process.

62. (new) The processing system of claim 61, wherein the processing system enters the isolated execution mode before loading the PE handler into the isolated memory area.

63. (new) The processing system of claim 61, further comprising:

a thread count storage, the processing system to store, in the thread count storage, a thread count indicating a number of threads operating in the isolated execution mode.

64. (new) The processing system of claim 63, further comprising:

an initialization storage, the processing system to update the thread count in response to access to the initialization storage.

65. (new) The processing system of claim 63, wherein the processing system provides indication of a failure mode in response to the thread count reaching a thread limit.

66. (new) The processing system of claim 61, further comprising:

a log storage to store identifiers of executive entities operating in the isolated execution mode.

67. (new) The processing system of claim 61, further comprising:

key storage to store a key to be used to handle one or more executive entities to operate in the isolated execution mode.

68. (new) The processing system of claim 67, wherein the key comprises data based on a substantially random value generated by a manufacture of hardware for the processing system.

69. (new) The processing system of claim 61, further comprising:

storage responsive to the processor; and

at least one executive entity encoded in the storage, the at least one executive entity selected from the group consisting of a processor executive (PE) and an operating system executive (OSE), the at least one executive entity to operate in the isolated execution mode.

70. (new) The processing system of claim 61, further comprising:

configuration storage to store a base value and a mask value, the processing system to establish the isolated memory area in the memory based at least in part on the base value and the mask value.

71. (new) The processing system of claim 61, wherein the PE handler storage comprises substantially non-volatile storage.

72. (new) A method comprising:

initializing a processing system during a boot process for the processing system, wherein the processing system comprises a processor and a memory, the processing system to support an isolated execution mode, a normal execution mode, a first privilege ring within the normal execution mode for use by an operating system (OS) kernel, and a second privilege ring within the normal execution mode for use by a software application;

during the boot process, establishing an isolated memory area in the memory, the isolated memory area to be inaccessible from the normal execution mode; and

after at least a portion of the processing system is initialized, loading a processor executive (PE) handler into the isolated memory area, the PE handler to manage, from the isolated execution mode, at least one subsequent operation in the boot process.

73. (new) The method of claim 72, wherein the processing system further comprises a chipset with a PE handler storage, the method further comprising:

obtaining at least part of the PE handler from the PE handler storage of the chipset.

74. (new) The method of claim 73, wherein the PE handler storage comprises substantially non-volatile storage.

75. (new) The method of claim 72, further comprising:

entering the isolated execution mode before loading the PE handler into the isolated memory area.

76. (new) The method of claim 72, wherein the processing system further comprises a thread count storage, the method further comprising:

storing a thread count in the thread count storage, the thread count indicating a number of threads operating in the isolated execution mode.

77. (new) The method of claim 76, further comprising:

providing indication of a failure mode in response to the thread count reaching a thread limit.

78. (new) The method of claim 76, wherein the processing system further comprises an initialization storage, the method further comprising:

updating the thread count in response to access to the initialization storage.

79. (new) The method of claim 72, further comprising:

operating one or more executive entities in the isolated execution mode; and

storing identifiers of the executive entities operating in the isolated execution mode.

80. (new) The method of claim 72, wherein the processing system comprises key storage to store a key, the method further comprising:

using the key to handle one or more executive entities to operate in the isolated execution mode.

81. (new) The method of claim 80, wherein the key comprises data based on a substantially random value generated by a manufacture of hardware for the processing system.

82. (new) The method of claim 72, further comprising

operating one or more executive entities in the isolated execution mode, wherein the executive entities comprise at least one entity selected from the group consisting of a processor executive (PE) and an operating system executive (OSE).

83. (new) The method of claim 72, wherein the processing system comprises configuration storage to store a base value and a mask value, and the operation of establishing an isolated memory area in the memory comprises:

using the base value and the mask value to establish the isolated memory area.

84. (new) An apparatus comprising:

a machine accessible medium; and

instructions encoded in the machine accessible medium, wherein the instructions, when executed by a processor of a processing system, perform operations comprising:

initializing at least part of the processing system during a boot process for the processing system, the processing system to support an isolated execution mode, a normal execution mode, a first privilege ring within the normal execution mode for use by an operating system (OS) kernel, and a second privilege ring within the normal execution mode for use by a software application;

during the boot process, establishing an isolated memory area in a memory of the processing system, the isolated memory area to be inaccessible from the normal execution mode; and

after at least a portion of the processing system is initialized, loading a processor executive (PE) handler into the isolated memory area, the PE handler to manage, from the isolated execution mode, at least one subsequent operation in the boot process.

85. (new) The apparatus of claim 84, wherein the processing system further comprises a chipset with a PE handler storage, and the instructions perform operations comprising:

obtaining at least part of the PE handler from the PE handler storage of the chipset.

86. (new) The apparatus of claim 84, wherein the instructions perform operations comprising:

causing the processor to enter the isolated execution mode before loading the PE handler into the isolated memory area.

87. (new) The apparatus of claim 84, wherein the processing system further comprises a thread count storage, and the instructions perform operations comprising:

storing a thread count in the thread count storage, the thread count indicating a number of threads operating in the isolated execution mode.

88. (new) The apparatus of claim 87, wherein the instructions perform operations comprising:

providing indication of a failure mode in response to the thread count reaching a thread limit.

89. (new) The apparatus of claim 87, wherein the processing system further comprises an initialization storage, and the instructions perform operations comprising:

updating the thread count in response to access to the initialization storage.

90. (new) The apparatus of claim 84, wherein the instructions perform operations comprising:

causing one or more executive entities to operate in the isolated execution mode; and

storing identifiers of the executive entities operating in the isolated execution mode.

91. (new) The apparatus of claim 84, wherein the processing system comprises key storage to store a key, and the instructions perform operations comprising:

using the key to handle one or more executive entities to operate in the isolated execution mode.

92. (new) The apparatus of claim 91, wherein the key comprises data based on a substantially random value generated by a manufacture of hardware for the processing system.

93. (new) The apparatus of claim 84, wherein the instructions perform operations comprising:

causing one or more executive entities to operate in the isolated execution mode, wherein the executive entities comprise at least one entity selected from the group consisting of a processor executive (PE) and an operating system executive (OSE).

94. (new) The apparatus of claim 84, wherein the processing system comprises configuration storage to store a base value and a mask value, and the operation of establishing an isolated memory area in the memory comprises:

using the base value and the mask value to establish the isolated memory area.